WHAT IS CLAIMED IS:

1. A security processing method comprising:

receiving, by a security processor, packets from a Gigabit Ethernet network;

processing at least a portion of the received packets, the processing consisting of at least one of the group of encrypting, decrypting and authenticating; and

transmitting, from the security processor, at least one result of the processing of the at least a portion of the received packets.

2. The method of claim 1 wherein processing comprises performing IPsec operations.

3. The method of claim 2 wherein the IPsec operations comprise adding or removing protocol elements.

4. The method of claim 1 wherein the at least a portion of the received packets comprise security association information for use in encrypting, decrypting or authenticating the at least a portion of the received packets.

5. The method of claim 1 further comprising the step of retrieving security association information from at least one data memory, wherein processing comprises encrypting, decrypting or authenticating the at least a portion of the received packets using the security association information.

6. The method of claim 1 wherein the at least a portion of the received packets comprise at least one reference to an address of a security association, the method comprising the step of retrieving security association information from at least one data memory according to the address, wherein processing comprises encrypting, decrypting or authenticating

at least a portion of the received packets using the security association information.

7. The method of claim 1 wherein the security processor comprises an integrated circuit.

8. A security processor comprising:

at least one Gigabit MAC; and

at least one processor, connected to send data to and receive data from the at least one Gigabit MAC, for encrypting, decrypting or authenticating at least a portion of the data.

9. The security processor of claim 8 wherein the at least one processor comprises at least one IPsec processor.

10. The security processor of claim 9 wherein the IPsec processor adds IPsec protocol elements to or removes IPsec protocol elements from the data.

11. The security processor of claim 8 further comprising at least one processor for processing at least one frame header from the received data to extract security association information.

12. The security processor of claim 8 further comprising at least one data memory for storing security association information for use by the at least one processor.

13. The security processor of claim 8 further comprising at least one processor that extracts security association information from data received from the at least one Gigabit MAC and that sends the security association information to the at least one processor.

14. The security processor of claim 8 further comprising at least one processor for:

extracting at least one address of at least one security association from data received from the at least one Gigabit MAC; and

sending the at least one address to the at least one processor;

wherein the at least one processor:

retrieves security association information from a data memory according to the at least one address; and

encrypts, decrypts or authenticates packets using the security association information.

15. The security processor of claim 8 wherein the security processor is an integrated circuit.

16. An in-line security processor comprising:

a plurality of Gigabit MACs; and

at least one processor, connected to receive data from at least one of the Gigabit MACs and to send data to at least one of the Gigabit MACs, for encrypting, decrypting or authenticating at least a portion of the data.

17. The in-line security processor of claim 16 wherein the at least one processor comprises at least one IPsec processor.

18. The in-line security processor of claim 17 wherein the IPsec processor adds IPsec protocol elements to or removes IPsec protocol elements from the data.

19. The in-line security processor of claim 16 further comprising at least one processor for processing at least one frame header from the received data to extract security

association information.

20. The in-line security processor of claim 16 further comprising at least one data memory for storing security association information for use by the at least one processor.

21. A security processing system comprising:

at least one media access controller;

at least one security processor; and

at least one switch for distributing or collecting packets between the at least one media access controller and the at least one security processor.

22. The security processing system of claim 21 wherein the at least one media access controller comprises at least one Gigabit MAC.

23. The security processing system of claim 21 further comprising at least one processor for allocating memory space associated with security associations used by the at least one security processor.

24. The security processing system of claim 21 wherein the at least one switch associates VLAN tags with the at least one media access controller.

25. The security processing system of claim 21 wherein the at least one media access controller sends packets comprising security association information to the at least one security processor.

26. The security processing system of claim 21 wherein:

the at least one media access controller sends packets comprising at least one address of at least one security association to the at least one security processor; and

the at least one security processor retrieves security association information from a data memory according to the at least one address and encrypts or authenticates packets using the security association information.

27. A chassis-based switch comprising:

at least one backplane;

at least one processing blade connected to the at least one backplane, the at least one processing blade comprising at least one media access controller; and

at least one switching blade connected to the at least one backplane, the at least one switching blade comprising:

at least one security processor; and

at least one switch for routing packets between the at least one media access controller and the at least one security processor.

28. A security processing system comprising:

at least one media access controller for:

executing TCP operations;

generating information associated with at least one security association; and

generating at least one packet including the information; and

at least one security processor, connected to receive the at least one packet from the at least one media access controller for:

locating the at least one security association using the information; and

encrypting, decrypting or authenticating data using the security association.

29. The system of claim 28 wherein the information comprises at least one address of the at least one security association.

30. The system of claim 28 wherein the at least one security processor generates an IPsec header using the information.

31. The system of claim 28 wherein the at least one media access controller derives the information from context information associated with the TCP operations.

32. The system of claim 28 wherein the at least one security processor is an integrated circuit and the at least one media access controller is an integrated circuit.

33. A security processing system comprising:

at least one Ethernet controller for:

executing TCP operations and storing context information associated with the TCP operations;

generating information associated with at least one security association from the context information; and

generating at least one packet including the information associated with at least one security association; and

at least one security processor, connected to receive the at least one packet from the at least one Ethernet controller for:

locating the at least one security association using the information associated with at least one security association; and

encrypting, decrypting or authenticating data using the security association.

34. A method of configuring a security processor comprising:

generating configuration information;

formatting the configuration information into at least one packet; and

sending the at least one packet over a Gigabit Ethernet network to a security processor.

35. The method of claim 34 wherein the at least one packet comprises at least one IPsec packet.

36. A method of configuring a security processor comprising:

receiving at least one packet containing configuration information over a Gigabit Ethernet network;

extracting the configuration information from the at least one packet; and

configuring a security processor using the extracted configuration information.

37. The method of claim 36 wherein the at least one packet comprises at least one IPsec packet.

38. A method of configuring a security processor comprising:

generating at least one security association;

formatting the at least one security association into at least one packet; and

sending the at least one packet over a Gigabit Ethernet network to a security processor.

39. A method of configuring a security processor comprising:

receiving at least one packet containing at least one security association over a Gigabit Ethernet network;

extracting the at least one security association from the at least one packet; and

storing the extracted at least one security association.

40. A method of generating a TCP frame comprising:

generating at least one header comprising an Ethernet header and a reference to an address of a security association; and appending the at least one header to an original TCP frame.

41. A method of processing a TCP frame comprising:

receiving a TCP frame according to an Ethernet header;

retrieving a security association from a data memory using to a reference to an address of a security association in the TCP frame; and

encrypting, decrypting or authenticating at least a portion of the TCP frame using the security association.

42. An in-line security processor comprising:

at least one MAC; and

at least one processor, connected to receive data from the at least one MAC and to send data to the at least one MAC, for encrypting, decrypting or authenticating at least a portion of the data.

43. The in-line security processor of claim 42 wherein the at least one processor comprises at least one IPsec processor.

44. The in-line security processor of claim 43 wherein the IPsec processor adds IPsec protocol elements to or removes IPsec protocol elements from the data.

45. The in-line security processor of claim 42 further comprising at least one data memory for storing security association information for use by the at least one processor.

46. The in-line security processor of claim 45 wherein

the at least one processor hashes at least a portion of the received data to extract at least one address of the security association information.

47. A security processing system comprising:
at least network controller; and
at least one security processor comprising:
at least one cryptographic processor; and
at least one MAC for sending packets to and receiving packets from the at least one network controller and for sending packets to and receiving packets from at least one network.

48. The security processing system of claim 47 wherein the at least one network controller adds information associated with at least one security association to at least a portion of the packets sent to the at least one security processor.

49. The security processing system of claim 47 wherein the at least one network controller adds at least one security header and trailer to at least a portion of the packets sent to the at least one security processor.

50. The security processing system of claim 49 wherein the at least one security processor modifies at least a portion of the at least one security header and trailer added by the at least one network controller.

51. The security processing system of claim 49 wherein the at least one security processor modifies at least one checksum in the at least one security header added by the at least one network controller.

52. The security processing system of claim 47 wherein

the at least one network controller modifies at least one maximum transmitted unit size in accordance with modifications the security processor makes to at least a portion of the packets.

53. The security processing system of claim 47 wherein the at least one network controller reduces at least one TCP/IP payload size in accordance with at least one security header and trailer size added to at least a portion of the packets.

54. The security processing system of claim 47 wherein the at least one security processor locates at least one security association according to a security parameter index contained in at least one packet received from the at least one network.

55. The security processing system of claim 47 wherein the at least one security processor locates at least one security association by hashing flow information from at least one packet received from the at least one network.

56. The security processing system of claim 47 wherein the at least one network controller securely communicates with the at least one security processor to configure the at least one security processor or retrieve status information from the at least one security processor.

57. A security processing method comprising:

receiving, by a security processor, packets from a network connection;

processing at least a portion of the received packets, the processing consisting of at least one of the group of encrypting, decrypting and authenticating; and

transmitting, from the security processor, over a network

connection, packets comprising at least one result of the processing of the at least a portion of the received packets.